Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate	)	CG Docket No. 17-59
Unlawful Robocalls	)	
	)	

COMMENTS OF TRANSACTION NETWORK SERVICES, INC.

Introduction

Transaction Network Services Inc. (TNS) has been delivering industry-leading solutions for the payments, financial and telecommunications industries since 1990. TNS is the preferred supplier of networking, integrated data and voice services to many leading organizations in the global payments and financial communities, as well as a provider of extensive telecommunications network solutions to service providers.

TNS manages some of the largest real-time community networks in the world, enabling industry participants to simply and securely interact and transact with other businesses, to access the data and applications they need, over managed and secure communications platforms. TNS' existing footprint supports millions of connections and provide access to critical databases. TNS' network securely blends private and public networking to enable customers to utilize a single connection for "one-to-many" and "many-to-many" connections over a global platform.

The TNS Call Guardian solution is a real time Telephone Number Reputation system currently deployed as part of a robocall solution by voice service providers who serve over 150 million subscribers. TNS' subsidiary company, Cequint, provides a mobile application that makes use of the Call Guardian reputation system as part of a total solution delivered to wireless service providers. TNS Call Guardian bases its reputational scoring on the observation of ~2 billion network events every day. TNS' broad view across the public switched telephone network, as a signaling and routing hub for over 400 providers, allows TNS an unparalleled view of malicious activity and the ability to score telephone number reputation in real time.

TNS provides comments in response to the Commission's NPRM as a partner to providers who seek to address the robocall problem.

Notice of Proposed Rulemaking

5. As a threshold matter, the Commission seek comment on how to define the term "illegal robocall" for purposes of this proceeding. Based on the Strike Force's recommendation, the Commission tentatively concludes that an "illegal robocall" is one that violates the requirements of the TCPA, the related Commission regulations implementing the Act, or the Telemarketing Sales Rule, as well as any call made for the purpose of defrauding a consumer, as prohibited under a variety of federal and state laws and regulations, including the federal Truth in Caller ID Act. Is this definition sufficient to capture all robocalls that should be subject to provider-initiated blocking? If not, how might the definition be expanded to serve the Commission's goals in this proceeding? For example, would this definition preclude voice service providers from blocking calls that are not lawful for other reasons, such as calls prohibited by an anti-stalking law or a court order, or preclude providers from blocking calls that violate a law but are not autodialed or prerecorded? Conversely, is this definition insufficiently precise so that it could lead to lawful calls being blocked? If so, what types of calls and how should the Commission change this definition?

TNS Comments:

Relative to provider-level blocking of illegal robocalls, the definition should include those calls that violate the Fair Debt Collections Practices Act. It is TNS' sense that it is better to err on the side of broad guidance, allowing providers to evolve as bad actors evolve, than to define problem robocalls narrowly. This is a self-policing issue for voice service providers. Blocking legitimate, desired calls will have negative customer consequences for the provider, and providers (and or their vendors) should have dispute resolution processes in place to address this.

Relative to subscriber-level blocking, the definition likely needs to be expanded to cover the pre-existing use case in which voice service providers' customers request that they not receive calls from specific telephone numbers. Providers block those calls at the request of customers today. This is a different use case from Section 6, below, where the Commission suggests the blocking of outbound calls from telephone numbers identified by subscribers to those numbers as inbound-only numbers (Do Not Originate numbers).

A. Blocking at the Request of the Subscriber to the Originating Number

6. *The 2016 Guidance PN made clear that voice service providers (whether providing such service through Time-Division Multiplexing, Voice over Internet Protocol (VoIP), or Commercial Mobile Radio Service) may block calls from a number if the subscriber to that telephone number requests such blocking in order to prevent its telephone number from being spoofed. The Bureau concluded that, where the subscriber did not consent to the number being spoofed, the call was very likely made with the intent to defraud, and therefore that no reasonable consumer would wish to receive such a call. Such calls are deemed to be presumptively spoofed and likely to violate the Commission's anti-spoofing rules, and have the potential to cause harm both to the called party and to the subscriber who uses the number. The Commission agrees with the Bureau's conclusions and propose to amend the Commission's rules to codify them, so as to provide increased certainty to providers. The Commission seeks comment on this proposal.*

TNS Comments: TNS supports the concept of a Do-Not-Originate (DNO) registry, and the Call Guardian solution is equipped to process such a list. We do, however, have some preliminary commentary on its requirements, and share those in order to contribute to further in-depth discussion.

1) The registry requires a centralized database. The responsibilities and liabilities of the registry must be clearly defined.
2) The entity chosen to operate such a registry must have experience in securely managing telco data with expertise in registry systems.
3) There needs to be a mechanism for businesses and other entities with telephone numbers appropriate for the registry to be made aware of the registry. Such entities will need to be authenticated before they can provide numbers to be blocked by the networks.
4) There must be a process defined for adding and removing numbers from the registry so it is kept current.
5) Processes and APIs must be defined so service providers can access the data.
6) Rules will need to be defined around participation. Will access to the registry be mandatory? Will there be repercussions for providers who do not block a

number contained within the DNO registry?

7. *The 2016 Guidance PN did not directly address issues related to providers sharing information about such subscriber requests. The Commission seeks comment on whether there are roadblocks to sharing information among providers necessary to effectuate subscriber requests for blocking and what, if any, rule changes or other measures are needed to ensure that such requests can be honored efficiently and effectively. Particularly, the Commission seeks comment on what measures, if any, the Commission should consider to facilitate the sharing of such requests among providers where, for example, the subscriber asks the provider that serves the number at issue to disseminate its request throughout the industry. The Commission notes that subscribers might not be readily able to identify each and every provider and to submit such a request to each provider individually. Although such information sharing at the subscriber's request appears to be consistent with the Commission's Customer Proprietary Network Information (CPNI) rules, the Commission seeks comment on whether there are remaining concerns that have not already been adequately addressed. Would such concerns, if any, be resolved by further clarification about the lawfulness of disclosing information to protect consumers and the network, and to prevent fraud? Are subscribers who request such blocking, absent instructions to the contrary, inherently requesting that that information be shared among providers, and does such sharing occur routinely, or are subscribers making multiple individual requests to multiple providers? Are there any particular concerns regarding the entity through which sharing occurs? For example, are there any specific concerns regarding sharing through an industry information or an entity involved in administering telephone numbers? The Commission notes especially that by seeking comment on these issues, and during the pendency of this proceeding, the Commission does not stall, interrupt, or prevent information sharing that is already occurring lawfully. Instead, the Commission asks whether the Commission can provide a better framework to facilitate and encourage sharing, and if so, how the Commission might do so.*

TNS Comments: Further discussion of the points raised in our response to Section 6 will likely yield a solution that will effectuate sharing of information in a manner that protects both voice call providers and their subscribers. A well-defined method of access to the Do-Not-Originate data, such as that which exists for other numbering systems such as 8XX Toll Free and Local Number Portability, will be required for reliability of this feature.

With respect to concerns about the entity through which sharing occurs, TNS is aware of the concern that certain entities providing robocall blocking solutions also have adjacent marketing insights or lead list lines of business, and that these adjacent services pose a risk to consumers, if they are a conduit for the consumers' information. There is acknowledged risk that these entities may play a role in feeding the problem they propose to solve.

TNS also believes that subscribers who request blocking of numbers understand that sharing of information may be required to effectively block problem calls. An update to terms and conditions of service would further clarify this point for providers' customers.

B. Calls Originating From Unassigned Numbers

8. *In the Strike Force Report, the Strike Force asked the Commission to further clarify that provider-initiated blocking is permissible where the call purports to originate from a number that the provider knows to be unassigned. As discussed in more detail below, use of an unassigned number is a strong indication that the calling party is spoofing the Caller ID to potentially defraud and harm a voice service subscriber. The Commission can readily identify three categories of unassigned numbers. Those categories are: (1) Numbers that are invalid under the North American Numbering Plan (NANP), including numbers with unassigned area codes; (2) numbers that have not been allocated by the North American Numbering Plan Administrator (NANPA) or the National Number Pool Administrator (PA) to any provider; and (3) numbers that the NANPA or PA has allocated to a provider, but are not currently assigned to a subscriber. The Commission seeks comment on rules to codify that providers may block numbers that fall into each of these three categories. The Commission seeks comment on how and when such blocking should be permitted and on whether there are other categories of numbers that should be considered to be unassigned.*

TNS Comments:

Blocking invalid, unallocated, or unassigned numbers makes good sense, and it is encouraging to see the Commission taking these important steps. TNS shares the following related points to address:

1) These numbers represent a small subset of the spoofing calls TNS sees across

its network. While there is a large number of unallocated telephone numberss (over 33million) that have been flagged as making calls, the volume of call activity from these numbers relative to all negative robocalling is very small. Based on our network insights, the focus of the NPRM on this subset of numbers has significant, but limited value.

2) TNS shares the Commission's concern that this change may result in greater incidence of spoofing of allocated numbers, creating a greater burden on individuals and businesses with whom those numbers are registered.
3) TNS' experience is that providers encounter challenges keeping published directories/subscriber lists up-to-date.
4) An Analytics Server will still be necessary.

   As the IETF and the FCC noted in October 2016, the role of an Analytics Server is a necessary component of an environment where no one solution is the silver bullet. TNS' Interaction with the PSTN allows our Call Guardian product to analyze and respond to bad actors as they emerge, and to return the reputation of telephone numbers that are the victims of spoofing once the spoofing has concluded.

   TNS emphasizes that real-time detection of caller reputation will remain an essential component of a complete solution. TNS Call Guardian has been very effective at identifying bad actors in real time, and, for this reason, TNS looks to the Commission to guard against rules that may prevent detection from evolving. It is possible that real-time detection is preferable to a solution that may result in bad actors increasingly spoofing legitimate telephone numbers.

C. Calls Originating From Invalid Numbers

9. *The Commission proposes to adopt a rule allowing provider-initiated blocking of calls purportedly originating from numbers that are not valid under the NANP. Examples of such numbers include numbers that use an unassigned area code; that use an N11 code, such as 911 or 411, in place of an area code; that do not contain the requisite number of digits; and that are a single digit repeated, such as 000-000-0000. Can providers, because of their intimate knowledge of the North American Numbering Plan, easily identify numbers that fall into this category? Further, because these numbers are not valid, there is no possibility that a subscriber legitimately could be originating calls from such numbers. Nor do the Commission foresee any reasonable possibility that a caller would spoof such a number for any legitimate, lawful purpose;*

for example, unlike a business spoofing Caller ID on outgoing calls to show its main call-back number, invalid numbers cannot be called back. The Commission therefore does not see a significant risk to network reliability in allowing providers to block this category of calls. The Commission seeks comment on this proposal.

TNS Comments: Please see comments under Section 8.

10. *More generally, the Commission seeks comment on whether, for purposes of this rule, to define invalid numbers more specifically than already described above. Further, the Commission seeks comment on what, if anything, the Commission can do to assist providers in correctly identifying invalid numbers. With regard to smaller providers, are there any particular measures the Commission or the numbering administrators can implement to assist them in more readily identifying or blocking calls originating from invalid numbers? Finally, the Commission seeks comment on any additional issues concerning the blocking of calls purportedly originating from invalid numbers.*

TNS Comments: It may be helpful for the Commission to aid in a campaign to raise awareness of the existence of a DNO registry in order to encourage businesses to sign up numbers that do not make outbound calls.

TNS believes the Commission may assist smaller providers by ensuring that guidance around solutions is not onerous. As the provider of an existing solution to smaller voice call providers, TNS understands their need for an effective solution that is easy to implement.

D. Calls Originating From Numbers Not Allocated to Any Provider

11. *The Commission also proposes to allow provider-initiated blocking of calls from numbers that are valid but have not yet been allocated by NANPA or the PA to any provider. Though these numbers are valid under the North American Numbering Plan, the Commission believes that they are similar to invalid numbers in that no subscriber can actually originate a call from any of them, and the Commission can foresee no legitimate, lawful reason to spoof such a number because they cannot be called back. The Commission seeks comment on this proposal.*

TNS Comments: Please see our response to Section 8. We are aware of some legitimate uses of call spoofing (calls from battered women's shelters are just one example). It may be onerous for legitimate spoofers to track numbers or number blocks that are unassigned.

12. *Unlike the category of calls described above, numbers in this category are not presumptively invalid. Instead, the provider must have knowledge that a certain block of numbers has not been allocated to any provider and therefore that the number being blocked could not have been assigned to a subscriber. The Commission seeks comment on whether providers can readily identify numbers that have yet to be allocated to any provider and, if not, whether the NANPA or PA could assist by providing this information in a timely, effective way. If there are difficulties in identifying unallocated numbers, the Commission asks commenters to provide specific descriptions and/or examples of any of those difficulties, and to offer any proposed solutions to overcome these difficulties. Can providers identify a subset of such number blocks, e.g., those shown as "available" by the PA? If providers can identify these number blocks, is there any delay in that information being updated or other factors that likely would result in calls from allocated numbers being blocked? If so, the Commission seeks comment on what steps are necessary to mitigate or eliminate the possibility of such calls being blocked. The Commission seeks comment on what further steps the Commission can take to assist providers, especially small providers, in identifying and blocking calls originating from numbers that have not been allocated to any provider and on any other relevant issues.*

TNS Comments: Assuming the numbering authorities do not identify any issues with sharing data about unallocated and unassigned blocks, the biggest issue will be the lag time from when such numbers are assigned and the mechanism to remove those numbers from blocklists. TNS has observed that there are both cases where unallocated numbers are used in violation of the TCPA, as well as cases where legitimate businesses are using telephone numbers that are not allocated to a provider. This update would affect both legitimate and illegitimate calling practices.

E. Calls Originating From Numbers That Are Allocated to a Provider, But Not Assigned to a Subscriber

13. *The Commission proposes to allow provider-initiated blocking of calls from numbers that have been allocated to a provider but are not assigned to a subscriber at the time of the call. Like the two categories of unassigned numbers discussed above, a* *subscriber cannot originate a call from such a number, and the Commission foresees no legitimate, lawful purpose for intentionally spoofing a number that is not assigned to a subscriber and thus cannot be called back. The Commission seeks comment on this proposal.*

TNS Comments: Please see our responses to Sections 8 and 12.

14. *Specifically, the Commission seeks comment on the ability of providers to accurately and timely identify numbers that fall within this category. The Commission believes that the provider to which a telephone number is allocated will know whether that telephone number is currently assigned to a subscriber. The Commission seeks comment on whether other providers can also determine, in a timely way, whether a specific telephone number is assigned to a subscriber at the time a specific call is made. Do providers currently share information about which numbers are assigned to a subscriber, and, if so, is such information shared in close to real time? Can the number portability database administered by the Number Portability Administration Center (NPAC) provide such information for a subset of numbers? Are there ways the Commission can facilitate or improve the sharing of information about numbers in this category? Should the Commission mandate the sharing of information about unassigned numbers to facilitate appropriate robocall blocking? If so, what is the most appropriate means to facilitate such information sharing?*

TNS Comments: In addition to the information provided in our response to Section 8, TNS notes that providers do share information through industry databases such as the Number Portability Administration Center (NPAC), the Line Information Database (LIDB), and other published directories. However, none of those data repositories contain a complete list of assigned numbers due to provider policy or application. Were this information shared, it would ease the ability to detect calls coming from unassigned telephone numbers. However, our experience indicates that it is challenging for providers to keep these lists up to date.

15. *If there are reasons that information about such numbers cannot be shared in an accurate and timely way, the Commission also seeks comment on whether a rule explicitly authorizing provider-initiated blocking of calls purportedly from numbers that are allocated to a provider but not assigned to a subscriber should apply only to the provider to which the number is allocated. Are there other factors that support or* *disfavor explicitly authorizing all providers to block calls purporting to originate from numbers in this category? Are there concerns for small providers, which presumably have a smaller set of allocated numbers than the larger providers? Finally, the Commission seeks comment on any issues not already raised that may arise by allowing providers to block allocated, but unassigned, telephone numbers.*

TNS Comments: TNS believes this concern may be better addressed with timely sharing of accurate information about allocation and subscription, perhaps allowing a third party to address inter-provider information sharing concerns. Were the provider of the number in question to be the only provider able to block calls for that number, the value of the initiative would be significantly diminished and would create a disadvantage for smaller providers.

F. Related Issues

16. *Internationally Originated Calls. The Commission notes that internationally originated calls may require special treatment. The Commission seeks comment on whether an internationally originated call purportedly originated from a NANP number should be subject to these rules, whereas an internationally originated call showing an international number would be beyond the scope of this rule. Are there any other special rules the Commission should consider with respect to internationally originated calls?*

TNS Comments: There may be cases of reputable international calls appearing with a NANP telephone number. Roamers, for example, may be problematic, under these rules, unless the Commission is limiting this restriction to unallocated numbers.

17. *Subscriber Consent. The Commission believes that no reasonable consumer would want to receive these calls. As a result, the Commission proposes not to require providers to obtain an opt-in from subscribers in order to block calls as described above. Obtaining opt-in consent from subscribers would add unnecessary burdens and complexity, and may not be technically feasible for some providers. The Commission seeks comment on this issue.*

TNS Comments: TNS is in agreement and, as such, does not believe customer opt-in for blocking of these types of calls should be required.

18. *Call Completion Rates. The Strike Force specifically requested that the Commission amend its rules to ensure that providers can block illegal calls without violating the call completion rules. Specifically, the Strike Force asked that these blocked calls not be counted for purposes of calculating a providers' call completion rate. The Commission proposes to exclude calls blocked in accordance with the rules the Commission adopts in this proceeding from calculation of providers' call completion rates and seek comment on that proposal.*

TNS Comments: TNS supports this recommendation.

Notice of Inquiry

19. *In the Strike Force Report, the Strike Force asked the Commission to clarify that providers are permitted to block "presumptively illegal" calls. Although the Commission agrees that no reasonable consumer would want to receive calls that are illegal, the Commission's call completion policies demand care in identifying such calls. The Commission believes that the criteria used to identify such calls must be objective, minimally intrusive on the legitimate privacy interests of the calling party, and must indicate with a reasonably high degree of certainty that a particular call is illegal. The Commission therefore seeks information on explicitly authorizing providers to block calls that are reasonably likely to be illegal based upon objective criteria in addition to the categories of unassigned numbers discussed above.*

TNS Comments: The Commission has done an excellent job of identifying types of calls that are clearly illegitimate and are candidates for blocking. However, as mentioned in our response to Section 8, this subset of problem callers is quite small. TNS has considerable insights into other mechanisms for identifying problem callers, some of which will not be addressed by STIR/SHAKEN. For this reason, it is our concern that this NPRM not limit either the scope or the ability of a solution that will serve as a reliable Analytics Server for real-time reputational information about callers. Providers must have the ability to block calls in good faith.

TNS, as mentioned in our response to Section 5, believes that voice call providers are incented to self-regulate, given that there are customer service repercussions for blocking good calls.

20. *The Commission believes that the categories of unassigned numbers discussed* *above exemplify objective standards for determining whether a specific call is illegal to a reasonably high degree of certainty. The Commission is aware, however, that there could be a variety of other objective standards that could indicate to a reasonably high degree of certainty that a call is illegal. Consequently, the Commission seeks comment on objective standards that would indicate to a reasonably high degree of certainty that a call is illegal and whether to adopt a safe harbor to give providers certainty that they will not be found in violation of the call completion and other Commission rules when they block calls based upon an application of objective standards. The Commission also seeks comment on ways that callers who make legitimate calls can guard against being blocked and to ensure that legitimate callers whose calls are blocked by mistake can prevent further blocking.*

TNS Comments: It is our experience that reliable real-time analysis based on a broad view of activity across the public switched telephone network (PSTN) provides the best safety net to address this concern. As noted, the majority of illegal robocall activity is originating from valid telephone numbers. Service providers must be able to use more sophisticated analytics to identify this activity. This real-time analysis differs significantly in value from solutions that depend on blacklists, which are not a scalable and are unable to determine reliably when to remove telephone numbers from the lists. There are similar issues with solutions that rely heavily on crowd-sourced information, *e.g.,* one provider recently shared that the telephone numbers on their subscribers' white and blacklists overlap 10%.

In addition, where STIR/SHAKEN will address part of this problem at the time when it is fully implemented, it will not address it in its entirety. For example, a caller may be using a telephone number for which it is legitimately the subscriber for annoying robocalling purposes.

With respect to legitimate callers being blocked by mistake, TNS has addressed this concern by implementing a Dispute Resolution process. The solution must rely on meaningful back-end knowledge, without which any bad actor could request that a number's reputation be adjusted.

A. Objective Standards To Identify Illegal Calls

21. *The Commission seeks comment on provider-initiated blocking based on objective criteria. The Commission seeks comment on what methods providers and third-party* *call blocking service providers employ in order to determine that a certain call is illegal. The Strike Force Report states that "[e]xamples of reasonable efforts include but are not limited to, soliciting and reviewing information from other carriers, performing historical and real time call analytics, making test calls, contacting the subscriber of the spoofed number, inspecting the media for a call (audio play back of the Real Time Protocol stream to understand the context of the call), and checking customer complaint sites." The Commission seeks more specific information regarding these and other methods or standards that can be used to identify illegal calls to a reasonably high degree of certainty.*

TNS Comments: TNS believes that detailed sharing of this information in a public document risks creating a blueprint for bad actors. TNS has considerable experience in this area, however there is risk in sharing this information outside of a closed industry forum.

22. *What other methods can be or are used? In particular, the Commission seeks comment on the extent to which information obtained through traceback efforts is, can, and should be used to identify future calls that are illegal to a reasonably high degree of certainty? The Commission asks commenters to submit information on whether some methods more accurately identify illegal calls in comparison to other methods, and whether some methods can identify unwanted calls but are less accurate in identifying illegal calls. Do certain methods work best in combination? Are some methods acceptable when used in the context of an informed consumer choosing to implement call blocking with knowledge of the risks of false positives, but might be less acceptable when used in the context of provider-initiated blocking? What can the Commission do to help providers minimize the possibility for false positives when blocking calls based on such methods?*

TNS Comments: Please see our response to Section 20, which comments on suitability of known solutions. TNS is in agreement with the IETF, SIP Forum, Robocall Strike Force, and others who have asserted that a layered approach is the best solution, and includes implementation of STIR/SHAKEN, an Analytics Server based on real-time reputational assessments, and a Do-Not-Originate (DNO) registry of numbers that do not make outbound calls.
Tracebacks offer value but are limited in terms of how specific the information about origin may be, and would require industry efforts to track down and address

bad actors that likely require additional discussion. Further, consumers must first become educated about the existence of tracebacks and the method for initiating a request.

In terms of specificity and reliability, with TNS Call Guardian, TNS has put a scoring system in place that grades confidence in assessment of problem calls, as opposed to a binary system, reducing the risk of false positives. TNS' provider customers use this system to customize which calls are blocked at the provider level versus at their customers' request. As mentioned in our response to Section 5, and throughout our responses, TNS believes that providers are incented to limit false positives based on their dedication to providing good customer service, and for this reason, TNS believes the Commission likely does not need to play a role in helping them to minimize false positives.

23. *Does provider size, geographic location, or other factors have an impact on which methods provide the most accurate results or which methods are feasible? What can the Commission do to provide support for smaller providers that wish to adopt these methods? Are some methods more likely to result in providers blocking legitimate calls in a manner that might violate the Act or the Commission's rules or polices related to call completion or that are more likely to contravene the policy goals underlying those rules? Calls that originate domestically may have differences from those which originate internationally, thus requiring consideration of different objective criteria. Are there any differences in how providers do, or should, handle calls originating outside of the United States in comparison to those originating domestically? If so, are there any limitations to a provider's ability to accurately identify the true origination point of a call?*

TNS Comments: Our data indicates that blacklist methods as well as those that depend on crowd-sourced data are often out of date, and are therefore more likely to result in false positives. This has been the case in email spam mitigation, as well. With respect to international calls, and known call-back schemes, we believe that Section 16 provides latitude to determine an approach that will permit providers to address this risk.

24. *The Commission recognizes that standards bodies have made significant progress on Caller ID Authentication Standards. The Commission applauds this progress, and* *encourages the industry to implement these standards as soon as they are capable of doing so. The Commission seeks comment on whether, once there is wide adoption of the protocols and specifications established by the Internet Engineering Task Force's (IETF) Secure Telephony Identity Revisited (STIR) working group and the Signature-based Handling of Asserted information using toKENs (SHAKEN) framework established in the joint Alliance for Telecommunications and Industry Solutions (ATIS) and Session Initiation Protocol (SIP) forum Network-to-Network Interconnection (NNI) Task Force, providers should then be permitted to block calls for which the Caller ID has not been authenticated. Should unauthenticated Caller ID alone be sufficient grounds for a provider to block a call, or should it be used only in combination with other methods? To what extent can these standards be implemented on networks using various types of technology? For example, will these standards work on VoIP calls and traditional wireline calls equally well? If not, how does that impact the propriety of blocking calls based on whether the Caller ID has been authenticated in accordance with these standards? Would it be possible to consider the lack of authenticated Caller ID only for those calls to which these industry standards can be applied? Are there special considerations related to implementing these standards on networks operated by small providers or in rural areas? What other factors should the Commission consider with regard to blocking calls based upon whether Caller ID has been authenticated in accordance with these standards?*

TNS Comments: TNS believes that unauthenticated Caller ID as eventually provided by STIR/SHAKEN will provide value, but will be best used in combination with other methods. Bad actors will evolve and continue to necessitate real-time analytics. Further, STIR/SHAKEN will be useful for SIP-to-SIP calls, uninterrupted along the network path, but will not be useful for calls that involve TDM wireline. Though the technical details of STIR/SHAKEN are well-defined, there are significant open business and policy issues which remain to be addressed.

As noted within IETF and SIP Forum documents, there will be entities who legitimately spoof Caller ID. For example, a customer service representative may appear to call from a company's toll-free number. These situations will require a mechanism to determine whether a group is asking for permission to spoof legitimately.

25. *The Commission seeks comment on whether sharing of information among* *providers can increase the effectiveness of call blocking methodologies and could enable small providers to benefit from the greater resources of larger providers that might be better able to create and implement more sophisticated methods of identifying illegal calls. The Commission seeks comment on these and any other impacts, positive and negative, of such information sharing and on what the Commission can do to encourage and facilitate such sharing of information in a manner most likely to result in accurate and timely identification of illegal calls. Again, the Commission notes that by seeking comment on these issues, the Commission does not stall, interrupt, or prevent information sharing that is already occurring lawfully. The Commission notes that section 222(d)(2) of the Act makes clear that CPNI may be shared "to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of . . . such services." The Commission seek comment on what other clarifications or rules changes, if any, would help to improve industry efforts to combat illegal robocalls and improve traceback efforts.*

TNS Comments: Due to providers' likely and justifiable reluctance to share information directly, it may make sense for a third party to act as a conduit.

B. Safe Harbor for the Blocking of Calls Identified Using Objective Standards

26. *The Commission also seeks comment on a broader safe harbor to provide certainty to providers that blocking calls in accordance with the rules the Commission adopts in this proceeding will not be deemed a violation of the Commission's rules and the Act, or counted for purposes of evaluating a provider's call completion rates. The Commission seeks comment on the appropriate scope of such a safe harbor.*

TNS Comments: As mentioned in our response to Section 5, and throughout, TNS believes that providers should be offered latitude with respect to safe harbor. Providers will not wish to block false positives, and are motivated to provide the best customer experience. Providers acting in good faith to deploy solutions to their end users should receive safe harbor protections.

In fact, it is TNS' belief that service providers already have some level of protection based on the amended section 230 of the Communications Act. Specifically, in Title II – Common Carriers, Part 1- Common Carrier Regulation, amended Section 230 Protection for Private Blocking and Screening of Offensive Material should be held to immunize (from civil liability) any provider of an interactive computer service (in this case a caller rating system and related application) that makes available to any registered user the technical means to empower a high level of individual user control over private blocking and screening of communications the user or provider believes to be fraudulent, unlawful, harassing, or otherwise objectionable (i.e. illegal and unwanted robocalls).

27. *The Commission seeks comment on what blocking practices and objective standards should be covered by any safe harbor. Are there any methods, practices, or objective standards that should expressly be excluded from the safe harbor? Are there methods, practices, or objective standards that warrant some protection, such as a rebuttable presumption that their use does not violate the call completion rules, but do not warrant the full protection of a safe harbor? What are they?*

TNS Comments: TNS suggests that solutions that introduce privacy concerns via the gathering and sharing of extraneous consumer information not expressly required for the core solution should be precluded from safe harbor. With respect to call completion rules, the Commission may decrease the chance of provider participation if it defines safe harbor narrowly.

28. *The Commission further seeks comment on how to formulate a safe harbor that avoids providing a roadmap enabling makers of illegal robocalls to circumvent call blocking by providers. Are there ways to provide both certainty to providers without providing a level of detail that would enable makers of illegal robocalls to circumvent blocking efforts? Should the Commission distinguish between standards that are general, e.g., regarding the presence or absence of Caller ID signatures, versus standards that involve patterns and statistics? Would it be workable to provide a safe harbor covering specific objective standards or specific objective standards implemented at some high threshold level but only a rebuttable presumption covering other objective standards or objective standards implemented at some low threshold? For example, what if the safe harbor applied when a provider blocks calls originating from a single number when the calls originating from that number per minute exceed a fairly high threshold, while a provider that applies a lower, non-public threshold would qualify only for a rebuttable presumption? Finally, should the safe harbor be the* *same for both large and small providers, and are there any considerations specific to small providers?*

TNS Comments: TNS believes that implementation of guidance around call blocking should not depend on revealing the mechanisms to determine the blocking. Safe harbor that dictates how a solution is deployed also does not permit providers to scale or evolve their solution as bad actor behavior changes. The presumption that providers are acting in the best interests of their customers is an important underpinning of safe harbor.

C. Protections for Legitimate Callers

29. *Even if providers use objective standards, there might be some situations in which legitimate calls would be blocked. For example, high-volume callers that properly obtain prior express consent might run afoul of call-per-minute restrictions even though all calls made are legal. This might occur if a call center lawfully spoofs the Caller ID on outgoing calls to utilize the business's toll-free number that consumers can use to call back or that might be familiar to consumers in a way that helps to identify the caller. The Commission seeks to avoid the blocking of such legitimate calls and, instead, seek to ensure that legitimate calls are completed. The Commission thus seeks comment on protections for legitimate callers. Specifically, should the Commission require providers to "white list" legitimate callers who give them advance notice? Should the Commission establish a challenge mechanism for callers who may have been blocked in error?*

TNS Comments: TNS has addressed this concern for its customers through a Dispute Resolution process, currently in place. A white list of legitimate callers will be difficult to protect and will become a target for spoofers. However, there is clearly value in establishing a list of schools, hospitals, emergency numbers, recall centers, flight alerts, etc. that have varying degrees of importance to call recipients. TNS has a mechanism in place to use information about important numbers, such as emergency services, in combination with real-time analytics to determine whether those numbers are the victims of spoofing.

30. *First, the Commission seeks comment on establishing a mechanism, such as a white list, to enable legitimate callers to proactively avoid having their calls blocked. Should the Commission specify the mechanism or mechanisms to be used or administrative* *details, such as the type of evidence providers might require of such legitimate callers? If so, what should the Commission require? Should the Commission specify a timeframe within which providers must add a legitimate caller to its white list? How should white list information be shared by providers? Is there anything the Commission can do to ensure that white list information is shared in a timely fashion such that legitimate callers need not contact each and every provider separately? Is Commission action needed to guard against white lists being accessed or obtained by makers of illegal robocalls? What is the risk that a caller could circumvent efforts to block illegal robocalls by spoofing numbers on the white list? Is this risk mitigated by the SHAKEN and STIR standards for authenticating Caller ID if, for example, the white list requires that all calls from the white listed telephone number be signed—once those standards have been implemented? Finally, the Commission seeks comment on any other relevant issues.*

TNS Comments: TNS does not believe that the FCC must specify the mechanism to determine the legitimacy of callers, nor a timeframe for adding those numbers to a whitelist, but it is possible that the FCC could be instrumental in gathering the numbers of emergency and other important services to distribute to solution providers. Were the Commission to provide excessive pressure or narrow guidance around this mechanism, the result may be the inadvertent addition of bad actors to a whitelist.

Again, TNS believes the risk of bad actors acquiring the list is high and for this reason emphasizes that analytics must overlay any white list efforts.

31. *Second, the Commission seeks comment on implementing a process to allow legitimate callers to notify providers when their calls are blocked and to require providers immediately to cease blocking calls when they learn that the calls are legitimate. How rapidly must a provider respond to a request to cease blocking, and should the Commission specify the information that providers must accept as proof that a caller is legitimate? Should the Commission require specific procedures, or allow providers discretion in how to develop processes, including processes for sharing and safeguarding this information? If provider discretion is allowed, should the Commission require providers to submit their procedures for staff review along with their objective standards? Are there procedures that would reduce any potentially undue burdens on smaller providers? The Commission believes most callers will contact their own provider first when their calls are being blocked. That provider,* *however, may not be the provider that is actually blocking the calls. The Commission seeks comment on how to facilitate information sharing so that the challenge reaches the provider actually blocking the calls. Finally, the Commission seeks comment on any other relevant issues.*

Lastly, the Commission seeks comment on whether providers should designate an officer or other authorized point of contact for legitimate callers seeking to proactively avoid having their calls blocked or to stop blocking of their calls. Would such a requirement represent an undue burden on smaller providers and, if so, what alternative should be available to legitimate callers?

TNS Comments: As mentioned in our responses to Sections 20 and 29, TNS has addressed provider concerns about false positives with its Dispute Resolution process. Because a solution exists today, TNS suggests that it would be preferable for the Commission to allow providers discretion in developing their own mechanism for addressing this concern.

TNS does not believe that FCC review of this mechanism should be required, and believes that a provider engaging in overly-aggressive blocking will experience customer service repercussions that supersede any need for regulation in this area. Finally, exposure of means and mechanisms may put place those mechanisms at risk for discovery by bad actors.